

1. Измените настройки STP таким образом, чтобы коммутатор Mikrotik-4 из резервного перешел в состояние рабочего.

Для изменения состояния порта коммутатора Mikrotik-4 в STP на «рабочий», нужно выполнить команду изменения приоритета порта, а затем активировать его: /interface bridge port set [find interface=имя_порта] priority=8192

2. Модель открытых систем OSI/ISO. Зачем она используется? Какие функции выполняются на уровнях 1 и 2?

Модель OSI (Open Systems Interconnection) используется для стандартизации процессов связи. На уровне 1 (физический) происходит передача битов по кабелям, а на уровне 2 (канальный) осуществляется управление доступом к среде передачи и проверка на ошибки.

3. Физический уровень технологии Ethernet. Какие физические среды используются для передачи сигнала? Как кодируется 0 и 1 в этих средах?

Физические среды Ethernet включают витую пару, коаксиальные кабели и оптоволокно. Кодирование 0 и 1 осуществляется с помощью различных сигналов (например, в витой паре - с помощью напряжения).

4. Коммутация Ethernet. Как устроены разъемы используемые для подключения витой пары и оптоволокна?

Разъемы для витой пары (RJ-45) и оптоволокна (LC, SC) отличаются количеством контактов и формой пазов для правильной установки.

5. Коммутация Ethernet. Какие стандарты существуют для расположения контактов в разъемах для подключения Ethernet по витой паре? В чем их разница? Почему синяя и зеленые пары в стандарте 568А (или оранжевая и синяя пары в стандарте 568В) расположены не последовательно друг за другом?

Стандарты T568A и T568B для витой пары определяют расположение контактов. Они отличаются тем, что порядок пар различается, чтобы минимизировать crosstalk. Синяя и зеленая пары не расположены последовательно для избежания помех.

6. Коммутация Ethernet. Какая максимальная длина кабеля витой пары может быть при подключении по технологии Ethernet? Какая максимальная длина оптоволоконного кабеля может быть при подключении по технологии Ethernet?

Максимальная длина витой пары в Ethernet — 100 метров, максимальная длина оптоволоконного кабеля может достигать нескольких километров, в зависимости от типа волокна и технологий.

7. Коммутация Ethernet. Возможно ли организация сети по технологии Ethernet без использования кабельного соединения? Если да, то какие физические среды могут быть использованы?

Да, возможна организация сети по технологии Ethernet без кабелей с использованием беспроводных технологий (например, Wi-Fi).

8. Для чего используется система VirtualBox?

VirtualBox используется для создания и управления виртуальными машинами, что позволяет тестировать ОС и программы без влияния на основную систему.

9. Какие два типа окон присутствуют в графическом интерфейсе VirtualBox? В чем из отличия?

В графическом интерфейсе VirtualBox существуют два типа окон: главное окно (управление виртуальными машинами) и окно консоли (интерфейс виртуальной машины). Главное окно отображает все доступные ВМ, а консоль предоставляет доступ к работающей ВМ.

10. Форматы файлов виртуальных носителей. Какие форматы поддерживаются в VirtualBox?

VirtualBox поддерживает форматы файлов виртуальных носителей, такие как VDI (VirtualBox Disk Image), VMDK (VMware Disk), VHD (Virtual Hard Disk) и другие. Если вам нужно больше информации, скажите! 

11. Типы доступа к виртуальным носителям

Типы доступа к виртуальным носителям в VirtualBox могут включать «с множественным подключением» (multiple connections) и «неизменяемый» (immutable).

С множественным подключением: это означает, что несколько виртуальных машин могут одновременно использовать один и тот же виртуальный носитель. Изменения, сделанные одной машиной, сохраняются и видны другим.

Неизменяемый: здесь носитель можно использовать только для чтения. Все изменения попадают в отдельный слой, и оригинал остается нетронутым. Это полезно для тестирования и сохранения состояния.

12. Коммутация сетей в VirtualBox

VirtualBox поддерживает несколько типов физических соединений:

NAT: виртуальная машина использует сеть хоста для доступа в интернет.

Сетевая мостовая связь: виртуальная машина напрямую подключается к сети хоста, как будто она физическое устройство.

Внутренняя сеть: машины могут обмениваться данными только между собой в рамках одной внутренней сети.

Сетевой шифратор (Host-only): виртуальная машина общается с хостом и другими ВМ, но не имеет доступа к внешней сети.

13. Режимы запуска виртуальных машин

Режимы запуска виртуальных машин:

Интерактивный режим: виртуальная машина запущена в окне, и пользователь может взаимодействовать с ней.

Фоновый режим: ВМ работает в фоновом режиме, без графического интерфейса.

Параметры управления осуществляются через командную строку или другие инструменты.

Консоль: это интерфейс, через который пользователь может управлять виртуальной машиной. В работах с консолью важно понимать, что нужно вводить команды точно, чтобы избежать ошибок.

14. HostKey в VirtualBox

HostKey — это сочетание клавиш, используемое для переключения между виртуальной машиной и хост-операционной системой. Это нужно, чтобы легко вернуть управление на хост, не останавливая ВМ.

15. Функции Wireshark

Wireshark выполняет множество функций, включая:

Захват пакетов с сетевого интерфейса.

Анализ и декодирование данных протоколов.

Просмотр информации о сетевых соединениях.

Фильтрация и сортировка трафика.

16. Изменение масштаба отображения в Wireshark

Масштаб отображения в Wireshark можно изменить с помощью колесика мыши или сочетаний клавиш Ctrl и +/- . Также можно использовать меню для изменения масштаба.

17. Включение/отключение разрешения имен

В Wireshark можно включить или отключить разрешение имен в меню "View" > "Name Resolution", где можно выбрать соответствующие параметры.

18. Сохранение и открытие захваченного потока пакетов

Чтобы сохранить поток пакетов в Wireshark, используйте "File" > "Save As...". Чтобы открыть ранее сохранённый файл, выберите "File" > "Open...".

19. Редактирование сохранённого потока пакетов

Wireshark не поддерживает редактирование пакетов непосредственно, но с помощью фильтров можно создать новый файл с нужными пакетами, используя "File" > "Export Specified Packets..." и задав нужные параметры фильтрации.

20. Фильтрация пакетов

Чтобы отфильтровать пакеты по протоколу DHCP, используйте фильтр: **bootp**. Для HTTP - фильтр: **http**.

21. Как в Wireshark создать типовой фильтр? Как его использовать? Чтобы создать типовой фильтр, вы можете использовать панель фильтров в верхней части интерфейса Wireshark. Введите ваше условие (например, **http**, **ip.addr == 192.168.1.1** и др.) и нажмите Enter. Фильтр будет применен к захваченным пакетам.

22. Как в Wireshark настроить интерфейс так, чтобы в процессе захвата потока пакетов курсор автоматически помещался на последний полученный пакет?

Перейдите в "View" > "Auto Scroll" и выберите "Scroll to Bottom on Packet Arrival". Это позволит вам автоматически перемещаться к последнему пакету при их получении.

23. Как в интерфейсе включить/отключить оформление цветом логически связанных пакетов? Перейдите в "View" > "Coloring Rules". Вы можете включить или отключить правила покраски, а также дополнительно изменять их.

24. Как в интерфейсе Wireshark посмотреть содержимое пакета? Можно ли увидеть вложенные составляющие в соответствии с моделью OSI/ISO? Выберите пакет в списке и посмотрите на содержащиеся в нем данные в нижней панели. Здесь вы сможете увидеть вложенные протоколы в виде дерева, что соответствует модели OSI.

25. Что такое МАС адрес? Зачем он используется? МАС-адрес (Media Access Control) — это уникальный идентификатор сетевого интерфейса для сетевых устройств. Он используется для идентификации устройства в локальной сети.

26. Определена ли какая-либо структура МАС-адреса? Что будет, если эту структуру не соблюдать? МАС-адрес состоит из 48 бит (6 байт), часто записываемых в виде шестнадцатеричных чисел, разделенных двоеточиями. Если структура не соблюдается, устройства могут не распознать адрес, что приведет к проблемам с соединением.

27. Допускается ли в одном сегменте сети два сетевых интерфейса с одинаковым МАС-адресом? Нет, это вызывает конфликты. Две сетевые карты с одинаковыми МАС-адресами в одном узле могут вызывать проблемы с определением пакетов в локальной сети.

28. Что такое «широковещательный» МАС-адрес? Зачем он используется? Есть ли еще какие-то служебные МАС-адреса? Широковещательный МАС-адрес — это **FF:FF:FF:FF:FF**, он используется для рассылки сообщений всем устройствам в сети. Существуют и другие специальные адреса, такие как мультикастовые адреса.

29. Как определить МАС адреса сетевых интерфейсов на маршрутизаторе Mikrotik? В операционной системе AstraLinux? На Mikrotik используйте команду в терминале: **/interface print**. В AstraLinux можно использовать команду **ifconfig** или **ip link**.

30. Возможно ли изменить эти МАС адреса? Если да, то как это сделать? Да, МАС-адреса можно изменить в настройках сетевого интерфейса. В Mikrotik это делается через интерфейс пользователя или команды, в Linux можно использовать **ifconfig eth0 hw ether 00:11:22:33:44:55**.

31. Что такое IP адрес? Как устроен IP адрес версии 4? Десятично-точечная нотация. IP адрес — это уникальный идентификатор, который назначается каждому устройству в сети, позволяющий отправлять и получать данные.

IP адреса версии 4 (IPv4) состоят из 32 бит, что делит адрес на четыре октета (по 8 бит в каждом). Каждый октет записывается в десятичной форме и разделяется точками, например: **192.168.1.1**. Каждый октет может принимать значения от 0 до 255. 

32. Структура пакета сетевого уровня для IPv4. Какие поля содержит?

Пакет IPv4 состоит из заголовка и полезной нагрузки. Заголовок включает следующие поля:

Версия (4 бита)
Длина заголовка (4 бита)
Услуга (8 бит)
Длина пакета (16 бит)
Идентификатор (16 бит)
Флаги (3 бита)
Смещение фрагмента (13 бит)
Время жизни (TTL, 8 бит)
Протокол (8 бит)
Контрольная сумма (16 бит)
IP-адрес источника (32 бита)
IP-адрес назначения (32 бита)
Дополнительные поля (если необходимо)

33. Пространство адресов IPv4. Группирование адресов. Классовая и бесклассовая адресация.

IPv4 использует 32-битные адреса, что дает 4,3 миллиарда уникальных адресов. Адреса могут быть сгруппированы в классы (A, B, C, D, E), и каждая группа имеет свои правила назначения.

Классовая адресация: определяет адреса на основе первых битов.

Бесклассовая адресация (CIDR): более гибкий подход, где адреса представляются с префиксом, например, /24.

34. Что такое маска сети и как она используется?

Маска сети — это 32-битное число, которое определяет, какая часть IP-адреса относится к сети, а какая — к устройству. Например, для адреса **192.168.1.0** и маски **255.255.255.0** адрес сети — это **192.168.1.0**.

Широковещательный адрес используется для отправки данных всем устройствам в сети. Нельзя назначить адрес сети или широковещательный адрес на узел. 

35. Как вычислить маску, если известно сколько адресов должно быть в подсети?

Чтобы вычислить маску:

Определите количество необходимых адресов (N).

Найдите наименьшую степень двойки, которая больше или равна N . Например, 32 адреса требуют маску /27 ($2^5 = 32$).

Если нужно уменьшить или увеличить количество подсетей, изменение маски (префикса) возможно. 

36. VLSM и CIDR - что это?

VLSM (Variable Length Subnet Mask) позволяет использовать маски различной длины для разных подсетей в одной сети.

CIDR (Classless Inter-Domain Routing) - бесклассовая адресация, которая позволяет более эффективно использовать адресное пространство.

Маска вида **1.2.3.4** — допустима, но чаще всего используются маски вида **255.255.255.0**. Запись вида **адрес/длина_префикса** указывает, сколько бит используется для обозначения сети.

37. Как связаны сетевой адрес и MAC-адрес? Протокол ARP.

Протокол ARP (Address Resolution Protocol) используется для преобразования IP-адресов в MAC-адреса. Сообщения ARP отправляются в одноадресном режиме (запросы) и многоадресном режиме (ответы).

Структура пакета ARP включает:

Тип аппарата

Тип протокола

Длина адреса

Операция (запрос/ответ)

MAC и IP-адреса источника и назначения.

38. Как принимается решение, какой MAC адрес использовать?

MAC-адреса определяются устройствами в сети. Специальные MAC-адреса используются для широковещательной передачи (например, FF:FF:FF:FF:FF:FF) или многоадресных рассылок. Примеры пакетов могут включать такие адреса в заголовках Ethernet.

39. Что произойдет, если в сети будут двум разным устройствам назначен одинаковый IPv4 адрес?

Это приведёт к конфликту адресов, и устройства не смогут правильно обмениваться данными, что вызовет проблемы в сетевом взаимодействии. 

40. Как посмотреть таблицу разрешенных IP адресов в устройствах?

Mikrotik: используйте команду /ip arp print в терминале.

Linux: команду arp -n или ip neighbor show.

Windows: команду arp -a в командной строке.

41. Можно ли добавить статические записи в таблицу MAC адресов? Если можно, то зачем это может потребоваться?

Да, статические записи можно добавлять в таблицу MAC-адресов. Это может потребоваться для следующих целей:

Устойчивость: Закрепление MAC-адреса за определённым портом, чтобы избежать его удаления из таблицы при изменениях в сети.

Безопасность: Защита от атак типа "ARP spoofing" путем фильтрации только заранее известных MAC-адресов.

Управление трафиком: Повышение производительности, так как необходимость в динамической обучении MAC-адресов уменьшается.

43. Как настраивается статическая адресация IPv4 в маршрутизаторе Mikrotik?

CLI:

```
/ip address add address=192.168.1.10/24 interface=ether1
```

Web-интерфейс:

Перейдите в раздел "IP" -> "Addresses".
Нажмите на "+" для добавления нового адреса.
Ведите IP-адрес и выберите интерфейс.
Нажмите "OK".

WinBox:

Откройте WinBox и подключитесь к маршрутизатору.
Перейдите в "IP" -> "Addresses".
Нажмите на "+" для добавления нового адреса.
Ведите необходимые данные и нажмите "OK".

44. Как вывести все назначенные IPv4 адреса на интерфейсах маршрутизатора Mikrotik?

В CLI:

```
/ip address print
```

Допускается ли назначение на один интерфейс нескольких адресов IPv4? Да, можно назначить на один интерфейс несколько адресов.

Должны ли быть это адреса из одного диапазона? Нет, адреса могут быть из разных диапазонов.

А из одного диапазона на разные интерфейсы? Да, это также допускается.

45. Как удалить назначенный IPv4 адрес в маршрутизаторе Mikrotik? А как изменить адрес? Маску?

Удаление адреса:

```
/ip address remove [find address=192.168.1.10]
```

Изменение адреса или маски:

```
/ip address set [find address=192.168.1.10] address=192.168.1.20/24
```

47. Как настраивается статическая адресация IPv4 в операционной системе AstraLinux?

В AstraLinux назначение IP-адреса можно выполнить через консоль. Команда для установки статического IP:

```
ip addr add 192.168.1.10/24 dev eth0
```

48. Как вывести все назначенные IPv4 адреса на сетевых интерфейсах AstraLinux?

Для вывода всех назначенных адресов:

```
ip addr show
```

49. Допускается ли назначение на один интерфейс нескольких адресов IPv4?

Да, это допускается.

Должны ли быть это адреса из одного диапазона? Нет, они могут быть из разных диапазонов.

Допускается ли назначить адреса из одного диапазона на разные интерфейсы? Да, это также возможно.

50. Как удалить назначенный IPv4 адрес в AstraLinux?

Для удаления адреса:

```
ip addr del 192.168.1.10/24 dev eth0
```

52. Протокол ICMP

ICMP (Internet Control Message Protocol) используется для передачи сообщений об ошибках и другой информации, касающейся IP-сетей. Основные типы сообщений ICMP включают:

Echo Request (Запрос эха): используется утилитой ping для проверки доступности хоста.

Echo Reply (Ответ на эхо): ответ на запрос эха.

53. Структура пакета ICMP

Структура пакета ICMP включает следующие поля:

Type: тип сообщения (например, 8 для echo request, 0 для echo reply).

Code: код уточняющий тип сообщения.

Checksum: контрольная сумма для обнаружения ошибок.

Identifier: идентификатор запроса.

Sequence Number: номер последовательности запроса.

Примеры пакетов можно захватить с помощью Wireshark или аналогичных инструментов. 

55. Принцип работы сетевого коммутатора

Сетевой коммутатор работает на уровне канального уровня (Layer 2) модели OSI. Он пересыпает данные между соединенными устройствами, используя таблицы MAC-адресов для определения, куда отправлять пакеты. Главное отличие от концентратора (hub) заключено в том, что коммутатор направляет пакеты только к нужному порту, а концентратор рассыпает их на все порты.

56. Таблица коммутации пакетов

Таблица коммутации содержит записи о MAC-адресах, связанных с каждым портом коммутатора. Она позволяет коммутатору эффективно направлять пакеты конкретному устройству, сокращая количество ненужного трафика в сети. Применение таблицы было заметно в различных практических заданиях, где сеть демонстрировала более высокую производительность.

57. Таблица коммутации и специальные MAC адреса

Специальные MAC-адреса, такие как широковещательные (ff:ff:ff:ff:ff:ff) и многоадресные, обрабатываются коммутатором иначе. Широковещательные пакеты рассыпаются на все порты, а многоадресные могут направляться на несколько определенных портов, в зависимости от группы, к которой относятся.

58. Коллизия

Коллизия происходит, когда два устройства пытаются одновременно отправить данные в сеть. В технологии Ethernet (CSMA/CD) разрешение коллизий происходит путем обнаружения конфликта и временной задержки отправки пакетов. **Домен коллизий** — это область сети, где могут происходить коллизии. Например, все устройства, подключенные к одному концентратору, образуют домен коллизий.

59. Широковещательный домен

Широковещательный домен — это область сети, в которой широковещательные сообщения могут быть приняты всеми устройствами. Он связан с доменом коллизий,

так как в одном широковещательном домене могут происходить коллизии, когда пакеты передаются по сетям с общими соединениями.

60. Разные диапазоны адресов в одном широковещательном домене

Как правило, в одном широковещательном домене не рекомендуется смешивать адреса из разных подсетей, так как это может привести к проблемам с маршрутизацией. Широковещательные сообщения отправляются всем устройствам в домене, и если они находятся в разных подсетях, это может вызвать путаницу и проблемы с сетевым трафиком.

62. Динамическое конфигурирование сетевых интерфейсов. Протокол DHCP, технология APIPA?

DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, который используется для автоматического назначения IP-адресов и других параметров конфигурации сетевых интерфейсов в компьютерной сети. **APIPA (Automatic Private IP Addressing)** — это технология, которая позволяет устройствам автоматически назначать себе IP-адреса в диапазоне 169.254.0.1 - 169.254.255.254, если DHCP-сервер недоступен.

63. Как происходит конфигурирование сетевого интерфейса по APIPA.

Если устройство не может получить IP-адрес через DHCP, оно автоматически выбирает случайный адрес из диапазона APIPA. Устройство проверяет, не используется ли этот адрес в сети. Если адрес свободен, он назначается устройству.

64. Типы сообщений в протоколе DHCP.

Существует несколько типов сообщений:

DHCPDISCOVER — запрос на получение IP-адреса.

DHCPOFFER — предложение IP-адреса от DHCP-сервера.

DHCPREQUEST — запрос на подтверждение IP-адреса.

DHCPCACK — подтверждение назначения IP-адреса клиенту.

DHCPNAK — отказ в назначении IP-адреса.

Дополнительно, **DHCPRELEASE**, **DHCPIINFORM**.

Режим передачи: Используется широковещательный режим для первых сообщений и одноадресный для подтверждения.

65. Возможна ли передача DHCP пакетов в одноадресном режиме?

Да, DHCP-пакеты могут передаваться в одноадресном режиме, когда клиент уже знает свой IP-адрес и отправляет запрос на конкретный DHCP-сервер для получения

параметров конфигурации. Это может использоваться в случае, если клиент получает адрес от сервера.

66. Что будет, если в сети установить два узла, на которых запустить DHCP сервер?

Если в сети присутствуют два DHCP-сервера, это может вызвать конфликты IP-адресов, так как оба сервера могут назначать одни и те же адреса разным клиентам, что приведет к проблемам с соединением и сетевым конфликтам.

67. Каковы условия конфигурирования DHCP сервера в сети?

Должен быть доступен IP-адрес для DHCP-сервера и диапазон адресов для раздачи. Необходимо настроить параметры, такие как шлюз, DNS-сервер и время аренды адресов.

DHCP-сервер должен быть подключен к сети, где клиенты могут его обнаружить.

68. Как организовать работу DHCP в сети без физического DHCP сервера?

Используется **DHCP Relay Agent**. Это промежуточное устройство, которое перенаправляет DHCP-запросы от клиентов к серверу, находящемуся в другой подсети. Один DHCP-сервер может обслуживать несколько подсетей через реле агентов.

69. Сетевой адрес IPv6. Структура.

IPv6 адрес состоит из 128 бит, записывается в виде восьми групп по 16 бит, разделенных двоеточиями (например, **2001:0db8:85a3:0000:0000:8a2e:0370:7334**).

Типы адресов:

Уникаст (Unicast) — для одного получателя.

Мульти cast (Multicast) — для группы получателей.

Эддресс любой (Anycast) — для ближайшего получателя.

Префикс — это часть адреса, которая используется для обозначения сети.

Способы сокращения записи: Например, **2001:0db8:0000:0000:0000:0000:0001** можно упростить до **2001:db8::1**.

70. Link-local адреса. Зачем используются?

Link-local адреса используются для связи устройств в одной сети без необходимости маршрутизации. Эти адреса имеют диапазон **FE80::/10** и могут использоваться для автоматического конфигурирования и соседского обнаружения.

71. Формирование интерфейсной части link-local адреса и EUI-64

Link-local адреса в IPv6 формируются на основе MAC-адреса устройства. Стандарт EUI-64 позволяет преобразовать 48-битный MAC-адрес в 64-битный идентификатор интерфейса. Этот процесс включает вставку **FFFF** в середину MAC-адреса и изменение одного бита (7-й бит) для создания уникального идентификатора.

Пример: Если MAC-адрес устройства: **00:1A:2B:3C:4D:5E**, то интерфейсная часть будет:

Изменяем: **00:1A:2B** на **02:1A:2B**.

Вставляем **FFFF**: **021A:2BFF:FE3C:4D5E**.

Получаем: **fe80::21a:2bff:fe3c:4d5e**.

72. Проверка связи с узлами через link-local адреса и идентификатор интерфейса

Связь с узлами можно проверить, используя утилиту **ping** с указанием link-local адреса. Однако нужно указывать идентификатор интерфейса, например, **ping fe80::21a:2bff:fe3c:4d5e%eth0**. Идентификатор интерфейса указывает, через какой сетевой интерфейс отправляется пакет.

73. Unique Local Unicast IPv6 адрес

Диапазон адресов: **fc00::/7**.

Назначение: Эти адреса предназначены для использования в частных сетях, подобно приватным IPv4-адресам. Они не маршрутизируются в интернете и могут использоваться для внутренней связи.

74. Global Unicast IPv6 адрес

Диапазон адресов: **2000::/3**.

Назначение: Эти адреса уникальны и могут маршрутизироваться в интернете, что позволяет устройствам в глобальной сети устанавливать соединения.

75. Специальные диапазоны адресов IPv6

::1: Мультикаст адрес для локального устройства (loopback).

::/128: Указывает на несуществующий адрес.

FF00::/8: Мультикаст адреса.

::ffff:0:0/96: Для совместимости с IPv4.

IPv6 имеет несколько специальных диапазонов адресов, каждый из которых имеет свое назначение. Вот основные из них:

Loopback адрес:

- **Адрес:** ::1
- **Назначение:** Используется для самопроверки устройства. Это аналог адреса 127.0.0.1 в IPv4.

Сылочный адрес:

- **Сначала 80 нулей:** ::FFFF:0:0/96
- **Назначение:** позволяет использованию IPv4-адресов в сетях IPv6, предоставляя совместимость для IPv4.

Мультикастовые адреса:

- **Диапазон:** FF00::/8
- **Назначение:** Используются для соединений мультикастом, позволяя отправлять пакеты группе узлов вместо одного конкретного.

Универсальные локальные адреса:

- **Диапазон:** FC00::/7
- **Назначение:** Частные адреса, используемые в локальных сетях. Эти адреса не маршрутизируются в Интернете.

Тестовые и резервные адреса:

- **Пример адреса:** 2001:DB8::/32
- **Назначение:** Резервированы для документации и примеров, чтобы избежать путаницы с реальными адресами.

Unspecified address:

- **Адрес:** ::
- **Назначение:** Используется для указания "неопределенного" адреса, когда адрес не известен или не применяется.

76. Протокол NDP (Neighbor Discovery Protocol)

Типы сообщений включают:

Router Solicitation (RS): Запрос на информацию о маршрутизаторах.

Router Advertisement (RA): Ответ на RS, содержащий информацию о маршрутизаторах.

Neighbor Solicitation (NS): Запрос о MAC-адресе устройства.

Neighbor Advertisement (NA): Ответ на NS.

77. Определение соседа с помощью NDP

С помощью сообщения Neighbor Solicitation (NS) можно узнать MAC-адрес устройства. Пример пакета может включать запрашиваемый IP-адрес и MAC-адрес отправителя, отправленный в multicast.

78. Статическая конфигурация IPv6 на маршрутизаторе Mikrotik

CLI:

Задать адрес: `/ipv6 address add address=2001:db8::1/64 interface=ether1`

Изменить: `/ipv6 address set [find address=2001:db8::1] address=2001:db8::2/64`

Удалить: `/ipv6 address remove [find address=2001:db8::2]`.

Web/WinBox: Интерфейс предоставляет форму для внесения изменений.

79. Статическая конфигурация IPv6 в AstraLinux

Задать адрес: В файле конфигурации сети `/etc/network/interfaces` добавьте строку.
`Plain
iface eth0 inet6 static
address 2001:db8::1
netmask 64`

Изменить/Удалить: Редактируйте этот файл соответствующим образом и перезапустите сетевой интерфейс.

80. Использование NDP при статической конфигурации IPv6

Протокол NDP автоматически обновляет таблицы ARP, когда в сети появляются новые устройства. Таким образом, даже при статической конфигурации, оставшиеся устройства смогут правильно определять MAC-адреса, обеспечивая корректную маршрутизацию пакетов.

81. SLAAC: Зачем используется? Как работает?

SLAAC (Stateless Address Autoconfiguration) используется для автоматической конфигурации IPv6-адресов, позволяя устройствам самостоятельно генерировать свои адреса без необходимости в DHCP-сервере. Он работает путём получения сетевых префиксов от маршрутизаторов, а затем по этому префиксу и MAC-адресу генерации уникального адреса.

82. SLAAC и протокол NDP

SLAAC использует Neighbor Discovery Protocol (NDP) для автоконфигурации адресов. Основные сообщения включают:

Router Solicitation (RS): Устройства запрашивают информацию о маршрутизаторах.

Router Advertisement (RA): Маршрутизаторы сообщают свои настройки, включая префиксы. Пример: устройство отправляет RS, а в ответ получает RA с префиксом и временем жизни.

83. Как долго сохраняются автоматически назначенные IPv6?

Автоматически назначенные адреса сохраняются до тех пор, пока устройство активно в сети. Информация о префиксах обычно распространяется каждые 200 секунд. Да, могут одновременно использоваться статически назначенные адреса и адреса, полученные по SLAAC.

84. MAC и IPv6 в NDP

В процессах NDP используется MAC-адрес для формирования IPv6-адреса через EUI-64, а также IPv6-адреса для обмена сообщениями. DAD (Duplicate Address Detection) проверяет, не занят ли уже адрес действующим устройством, отправляя Neighbor Solicitation и ожидая ответа.

85. Один IPv6 адрес на нескольких интерфейсах?

Один IPv6-адрес нельзя назначить сразу многим интерфейсам на одном узле, так как это приведет к конфликтам в маршрутизации. Однако можно настроить адреса на разных интерфейсах, но они должны быть уникальными.

86. Протокол ICMPv6

ICMPv6 — это расширение ICMP для IPv6. Он включает новые типы сообщений, такие как Router Solicitation и Router Advertisement, а также Neighbor Solicitation и Neighbor Advertisement. У пакетов ICMPv6 более сложная структура, включающая заголовки для идентификации типа сообщения и соответствующих данных.

87. DHCPv6: Типы сообщений, структура пакета

DHCPv6 включает типы сообщений, такие как Relay-Forward, Relay-Reply, Solicitation, Advertisement, Request и Reply. Структура пакета включает заголовок с типами сообщений и параметры, такие как идентификаторы клиентских и серверных сообщений.

88. Связь DHCP и SLAAC

DHCP и SLAAC могут использоваться вместе. SLAAC автоматически настраивает адреса, а DHCPv6 может использоваться для получения других параметров конфигурации, таких как DNS-серверы.

89. Настройка DHCP на маршрутизаторах Mikrotik: DHCP-Client

На Mikrotik DHCP-клиент настраивается через интерфейс или терминал. Это позволяет маршрутизатору получать адрес и сетевые настройки от DHCP-сервера в сети для доступа к интернету.

90. Настройка DHCP на маршрутизаторах Mikrotik: DHCP-Server

DHCP-сервер на маршрутизаторе Mikrotik предоставляет IP-адреса и настройки клиентам в локальной сети. Он упрощает управление сетевыми адресами и позволяет автоматизировать процесс подключения новых устройств.

91. Настройка DHCP в AstraLinux. DHCP-Client.

DHCP-клиент в AstraLinux настраивается обычно через конфигурационный файл `/etc/dhcp/dhclient.conf`. Вам нужно будет включить соответствующие параметры для получения IP-адреса автоматически.

92. Настройка DHCP в AstraLinux. DHCP-Server.

Для настройки DHCP-сервера в AstraLinux необходимо установить пакет `isc-dhcp-server`, настроить файл конфигурации `/etc/dhcp/dhcpd.conf`, определив диапазон адресов, время аренды и другие параметры.

93. DHCPv6 и NDP. Используются совместно?

Да, DHCPv6 и NDP (Neighbor Discovery Protocol) используют совместно, чтобы обеспечить автоматическую конфигурацию IP-адресов и управление соседями в IPv6-сетях. NDP помогает в обнаружении других устройств в сети, а DHCPv6 — в динамической передаче IP-адресов.

94. Что такое сетевой маршрут? Таблица маршрутов? Сколько таблиц маршрутов может быть на одном узле?

Сетевой маршрут — это путь, по которому передаются данные от одного узла к другому. Таблица маршрутов — это структура данных, содержащая маршруты к различным сетям. На одном узле может быть несколько таблиц маршрутов, особенно в сложных сетевых конфигурациях.

95. Технология CIDR. Как и зачем она используется в маршрутизаторах?

CIDR (Classless Inter-Domain Routing) позволяет более эффективно управлять адресным пространством, используя маски подсети переменной длины. Это уменьшает количество записей в таблицах маршрутизации и позволяет лучше использовать IP-адреса.

96. Статическая маршрутизация. Процесс определения маршрута для передачи пакета. Маршрут «по умолчанию». Политика маршрутизации.

Статическая маршрутизация предполагает ручное определение маршрутов в таблице маршрутизации. Маршрут "по умолчанию" используется, когда нет других маршрутов для передачи пакетов. Политика маршрутизации — это набор правил, определяющий, как выбирать маршруты.

97. Алгоритм поиска проблем с маршрутизацией.

Проверка подключения к шлюзу.

Проверка таблицы маршрутизации.

Тестирование ping для конечных устройств.

Анализ трассировки маршрута (traceroute).

98. Как получить информацию о таблице(ах) маршрутизации для IPv4 и IPv6 на маршрутизаторе Mikrotik, в операционной системе AstraLinux.

На Mikrotik: используйте команду `/ip route print` для IPv4 и `/routing/ipv6/route/print` для IPv6.

В AstraLinux: используйте `ip route show` для IPv4 и `ip -6 route show` для IPv6.

99. Динамическая маршрутизация. Зачем используется? Виды протоколов динамической маршрутизации.

Динамическая маршрутизация автоматически обновляет таблицы маршрутизации и адаптируется к изменениям сети. Основные виды протоколов: RIP, OSPF, EIGRP, BGP.

100. Протокол динамической маршрутизации RIP. Принцип работы. Версии протокола. Структура используемых пакетов.

RIP использует алгоритм "ближайшего соседа", обновляя таблицы маршрутизации каждые 30 секунд. Версии: RIP v1 и RIP v2. Структура пакета включает адрес назначения, метрику и информацию о маршруте.

101. Протокол динамической маршрутизации OSPF. Принцип работы. Версии протокола. Структура используемых пакетов. Понятие «область обмена маршрутами».

OSPF использует алгоритм Dijkstra для нахождения кратчайшего пути. Области маршрутов помогают делить большую сеть на подъемы, уменьшая нагрузку. Версии: OSPFv2 и OSPFv3.

102. Интеграция данных между протоколами RIP и OSPF. Возможна ли? Приведите пример применения такой интеграции.

Интеграция возможна через маршрутизаторы, поддерживающие оба протокола. Например, можно настроить RIP для обмена маршрутами с OSPF на границе двух сетей.

103. Настройки ядра операционной системы Linux. Переменные net.ipv4.ip_forward и net.ipv4.conf.all.rp_filter. Зачем нужны? Какие ещё переменные используются?

`net.ipv4.ip_forward` включает пересылку пакетов между интерфейсами.
`net.ipv4.conf.all.rp_filter` усиливает безопасность, предотвращая подделку IP-адресов. Используются и другие переменные, как `net.ipv4.conf.all.accept_redirects`.

104. Что такое фильтрация сетевых пакетов? Зачем используется? Приведите примеры.

Фильтрация сетевых пакетов — это процесс анализа и фильтрации сетевых данных для блокировки или разрешения трафика. Примеры: блокировка специфических IP-адресов, разрешение пакетов только для определенных портов.

105. Как настроить фильтрацию пакетов в маршрутизаторах Mikrotik.

Используйте Winbox или командной строки для создания правил фильтрации в разделе IP > Firewall.

106. Как настроить фильтрацию пакетов в операционной системе AstraLinux?

Используйте `iptables` или `nftables`, добавляя правила для разрешения или блокировки трафика.

107. Что такое трансляция сетевых адресов? Типы трансляции? Какие проблемы возникают при трансляции адресов?

Трансляция сетевых адресов (NAT) позволяет скрыть внутренние IP-адреса за одним публичным адресом. Основные типы: статическая, динамическая и PAT. Проблемы: сложности с сетевым мониторингом и несовместимость с некоторыми протоколами.

108. Как настроить трансляцию адресов в маршрутизаторах Mikrotik.

Используйте Winbox, создавая правило в разделе IP > Firewall > NAT.

109. Как настроить трансляцию адресов в операционной системе AstraLinux?

Используйте `iptables`, добавляя правила для NAT.

110. Модель OSI/ISO. Канальный и сетевой уровни: отличия и пример использования.

Модель OSI делит сетевые функции на 7 уровней. Канальный уровень отвечает за передачу данных между непосредственно связанными устройствами, тогда как сетевой уровень управляет маршрутизацией данных между различными сетями. Например, Ethernet работает на канальном уровне, а IP — на сетевом.

111. Как работают сетевой коммутатор, сетевой концентратор, сетевой мост?

Сетевой концентратор (хаб) принимает данные от одного устройства и отправляет их всем другим устройствам в сети. Он не фильтрует или обрабатывает данные, используемый в простых локальных сетях (LAN).

Сетевой мост (бридж) соединяет две или более сетевые сегменты, фильтруя трафик и снижая количество коллизий, передавая информацию только на те порты, где находятся целевые устройства.

Сетевой коммутатор (свитч) динамически управляет данными, отправляя их только конкретным устройствам на основе адресов MAC. Это повышает эффективность передачи данных и производительность сети.

112. Зачем используются сетевые мосты в маршрутизаторах?

Сетевые мосты помогают соединять разные сегменты сети, они могут работать в режиме "моста" для повышения производительности и управления трафиком.

Применяется на практике для разделения сетей по разным стандартам (например, PoE, Wi-Fi). Пример: в крупной организации, где сетевой организуется через разные этажи, мосты помогают соединить несколько локальных сетей в единую и управляемую.

113. Как настроить сетевой мост в маршрутизаторе Mikrotik? В AstraLinux?

Чтобы настроить мост в MikroTik:

Зайти в интерфейс WinBox или WebFig.

Перейти в раздел "Bridge".

Создать новый мост, добавив интерфейсы, которые необходимо объединить.

В AstraLinux это можно сделать через командную строку с помощью утилиты **bridge**, например:

```
ip link add name br0 type bridge  
ip link set dev eth0 master br0  
ip link set dev eth1 master br0
```

```
ip link set br0 up
```

114. Что такое цифровой шторм? Как от него защититься?

Цифровой шторм — это перегрузка сетевого трафика, вызванная внезапным увеличением запросов, что может привести к отказу в обслуживании (DoS). Защита включает настройку лимитов на трафик, использование систем обнаружения вторжений (IDS) и управление трафиком через брандмауэр.

115. Протокол определения колец STP. Зачем используется?

STP (Spanning Tree Protocol) предотвращает петли в сетях с избыточными соединениями. Он работает по принципу определения определенного "корневого" коммутатора и блокирует порты, создающие петли. Основные версии:

802.1D (стандартный)
Rapid STP (RSTP, 802.1w)
Multiple STP (MSTP, 802.1s)

116. Всегда ли обязательно использовать STP?

Не всегда. Плюсы включают защиту от петель, а минусы — задержки при переключении и сложность управления. Некоторые варианты сети могут обходиться без STP, если структуры сети не имеют избыточности.

117. Виртуальные локальные сети (VLAN): стандарт, зачем используются?

VLAN позволяют сегментировать сеть, создавая логические подгруппы в пределах одной физической сети. Это улучшает безопасность и управление трафиком. Например, в школе разные классы могут быть в отдельных VLAN для поиска данных. Максимальное количество VLAN в сети — 4096.

118. Могут ли быть одинаковые идентификаторы VLAN для разных портов маршрутизаторов?

Да, идентификаторы VLAN могут повторяться на разных устройствах, но это будут разные локальные сети. На одном коммутаторе или маршрутизаторе идентификаторы должны быть уникальными.

119. Как настроить в маршрутизаторе Mikrotik виртуальные интерфейсы для обработки тегированных пакетов?

Зайти в WinBox.

Перейти в "Interfaces".

Создать новый интерфейс типа "VLAN".

Указать нужный ID VLAN и интерфейс.

120. Как настроить в AstraLinux виртуальные интерфейс для обработки тегированных пакетов?

Пример настройки через командную строку:

```
ip link add link eth0 name eth0.10 type vlan id 10
```

```
ip link set dev eth0.10 up
```

Это создаст виртуальный интерфейс для обработки трафика VLAN с ID 10.